Horváth Attila

A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai I. rész

(A biztonság változó értelmezése)

DOI 10.17047/HADTUD.2016.26.E.189

Absztrakt:
A tanulmány az utóbbi évtizedekben megváltozott felfogások alapján áttekinti a biztonságot veszélyeztető kockázati tényezőket. A szerző korábbi kutatásaira alapozva és az újabb kutatások eredményeként a tanulmány részletesen elemzi a kritikus infrastruktúrák (létfontosságú rendszerelemek) működésével kapcsolatos veszélyeket. A létfontosságú rendszerelemek kölcsönhatásainak vizsgálatával bizonyítja egy átfogó biztonsági szemlélet elterjesztésének szükségességét. A szerző az új típusú biztonsági kockázatok közül a mesterséges intelligenciák társadalmi, katonai és etikai kockázatait vizsgálja.
Kulcsszavak:
biztonság; kritikus infrastruktúra védelem; kockázatok.

Horváth, Attila

New Risks of Critical Infrastructure and Technological Development. Part I.

(Changing Interpretation of Security)

Abstract:
This study reviews the factors of security risks, in the light of the changing perceptions in the last decades. It analyses the hazards for the operation of critical infrastructure systems in detail, based on the previous and current research results by the author. With the investigation on the interactions between critical systems elements, he provides the evidence for the necessity of spreading a comprehensive security approach. Among the new type of security hazards, the author examines the societal, military and ethical risks relevant with the appearance of artificial intelligence.
Key words:
Security; Critical Infrastructure Protection; Risks.

Mindazok számára, akik a hidegháború végén megélték a két világrendszer felbomlását, a váratlan és viszonylag gyorsan bekövetkező történelmi események örök élményt jelentettek. A várt biztonságos „szép új világ” azonban sokak várakozása ellenére nem jött el. A társadalomtudósok és a biztonságért felelős politikusok körében általánosan elfogadottá vált az a megállapítás, hogy a bipoláris világrend idején a két szembenálló szuperhatalom: az Amerikai Egyesült Államok (a továbbiakban: Egyesült Államok), valamint a Szovjetunió és szövetségeseik által mesterségesen kontroll alatt tartott biztonsági kockázatok jelentettek igazán komoly veszélyt a Föld lakói számára.

A két világrendszer közötti rivalizálás megszűnése elhárította az akadályt a globalizáció térnyerése elől, amelyet később egy hihetetlen gyors tempójú infokommunikációs forradalom is elősegített. Ez a sokak által „gyűlölt és szeretett” globalizáció és az információ-technológiai fejlődés újabb kockázatok megjelenését eredményezte, amelyek komoly fenyegetést jelentenek a biztonságra is.

A tanulmányomban az úgynevezett *kritikus infrastruktúrák és a technológiai fejlődés biztonsági kihívásaival* foglalkozom. A kockázati tényezők tárgyalásakor nem törekszem a teljességre.

A biztonság értelmezésének változásai. A kritikus infrastruktúra védelem előtérbe kerülése

A második világháború után a biztonsági tanulmányok és a biztonságpolitikai elemzések középpontjában továbbra is a katonai és külpolitikai kérdések álltak. A hidegháborút követően azonban a kutatások és elemzések más jellegű kockázatok vizsgálatára is nyitottabbá váltak.[1] Ez azt jelentette, hogy a katonai és a geopolitikai kérdések elemzése továbbra is fontos maradt a kutatók és a döntéshozók számára, de megszűnt azok kizárólagossága.

A különböző kutatóintézetek olyan megnövekedett kockázatokkal kapcsolatos elemzéseket publikáltak, mint például az etnikai-vallási ellentétek felerősödése, vagy a meggyengült, cselekvőképtelen államok működésképtelensége, a terrorizmus, a szervezett bűnözés, a kábítószer-kereskedelem, az illegális fegyverkereskedelem.[2]

A teljesség igénye nélkül az olvasók figyelmét szeretném felhívni arra, hogy az 1990-es években számtalan olyan esemény következett be, amely lekötötte a biztonságpolitikával foglalkozó kutatók figyelmét. Megszűnt a Varsói Szerződés, felbomlott a Szovjetunió, majdnem egy évtizedig elhúzódó háború tört ki a volt Jugoszlávia területén, szégyenletes népirtás történt Ruandában, Algériában felerősödött a szélsőséges iszlamista terrorcsoportok tevékenysége, valamint erre az időszakra tehető a szélsőséges iszlamista terroristahálózat, az Al-Kaida megerősödése is.

A kétpólusú világrend felbomlását követően a fegyveres küzdelem tartalma is jelentős átalakuláson ment át. Ma már nem az a jellemző, hogy hadtestek, hadseregek és hadseregcsoportok állnak egymással szemben (bár ezt sem lehet teljesen kizárni). Egyre inkább elterjedt az *irregurális hadviselés*. Az állami felügyelet alatt tartott nemzeti haderőknek koalíciós, többnemzeti szövetségi keretekben kell fegyveres küzdelmet, válságkezelő műveleteket folytatni terrorcsoportok, gerillák, félkatonai szervezetek magánhadseregek vagy bűnszervezetek ellen.[3]

A biztonságpolitikában és a hadtudományban napjainkra olyan kifejezések honosodtak meg, mint az *aszimmetrikus* vagy a *hibrid hadviselés*. A helyzet bonyolultságát jól szemlélteti az Iraki és Levantei Iszlám Állam (ISIL) elleni küzdelem, de az ISIL ellen a harcoló erők jellemzése is kihívást jelent.[4] Nem vállalkozik könnyű

[1] Walt, M. Stephen: A biztonsági tanulmányok reneszánsza. In.: Póti László (szerk.): Nemzetközi biztonsági tanulmányok. Zrínyi Kiadó, Budapest, 2006. pp. 9–52.

[2] Horváth Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. In.: Horváth, Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből I., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 25–48.

[3] Porkoláb Imre: Hibrid hadviselés: új hadviselése forma, vagy régi ismerős. Hadtudomány, 2015/3-4. szám. pp. 36–48.

[4] Erről a kérdésről lásd bővebben: Kis-Benedek József: Az Iraki és Levantei Iszlám Állam (ISIL) és az ellene folytatott küzdelem tendenciái. Hadtudomány, 2016/1–2. szám. pp. 29–39. Cikkében a szerző azt is kifejti, hogy az ISIL egy olyan gerillaszervezet, amely terroristamódszereket alkalmaz, és amelynek államalapítási szándékai vannak.

feladatra az, aki meg akarja válaszolni a fegyveres konfliktusok alapvető kérdését, hogy *ki kivel* van. [5]

Még a két világrendszer felbomlása előtt a biztonsági tanulmányok elismert kutatói körében élénk szakmai vita kezdődött arról, hogy a biztonság tárgyát szükséges-e kibővíteni a geopolitikai, katonai kérdések körén túl. A „tradicionalista" álláspontra helyezkedők azt hangoztatták, hogy a biztonság fogalmának kiszélesítése azt eredményezi, hogy a bővebb értelmezés alkalmazásakor elvész majd a lényeg. Vagyis az új módszertannal nem lehet meghatározni a főbb kockázatokat. A „bővítők" csoportjába tartozók viszont azt hangsúlyozták, hogy a biztonság értelmezése már nem korlátozódhat a katonai erőegyensúllyal, illetve a kormányzati döntések előkészítésével kapcsolatos kérdések elemzésére.[6]

A brit Barry Buzan professzor vezette úgynevezett Koppenhágai Iskola kutatói több terület „biztonságosítását" tartották szükségesnek. Néhány ágazatot meg is neveztek, de ennél sokkal fontosabb, hogy a kutatók olyan kritériumok bevezetését javasolták, amelyekkel a kormányok és a nemzetközi szervezetek napjainkig azonosulni tudtak. A Buzan-vezette kutatócsoport ajánlásai szerint azokat a problémaköröket sorolhatjuk a biztonság kategóriájához, amelyekkel kapcsolatban felmerülhet az anyagi és létfenyegetettség ténye, illetve a hozzájuk kapcsolható kockázati elemek kezeléséhez rendkívüli (kormányzati) intézkedések meghozatala szükséges. [7]

A biztonsággal kapcsolatos kérdések folyamatos értelmezése azért is szükséges, mert a posztmodern társadalom kialakulása, a globalizmus kiszélesedése és a felgyorsult technológiai fejlődés olyan civilizációs kihívásokkal jár együtt, amelyek felkeltették a szellemi-tudományos közélet kiemelkedő képviselőinek az érdeklődését is.

A XX. század végén jellemző gondolkodás egyik fenegyerekének és különcének számító Jean Baudrillard olyan veszélyekre hívta fel a figyelmet, amelyek a globális felmelegedés hatásaival, a természeti katasztrófákkal, a géntérképek elkészítésével, valamint a telekommunikációs forradalom eredményeivel kapcsolatosak.[8] Korunk gondolkodó emberének nem igazán kell magyarázni az információs technológia kockázatait, arra viszont már valószínűleg nagyon kevesen emlékeznek, hogy 1999 és 2000 fordulóján milyen előkészületeket kellett tenni azért, hogy a telekommunikációs rendszerek és hálózatok működőképesek maradjanak. Az állami és a magánszektor minden területén fel kellett készülni az informatikai rendszerek esetleges leállására vagy működési zavaraira.

A közelmúltban Stephen W. Hawking, a világhírű, Wolf-díjas brit fizikus arra hívta fel a figyelmet, hogy a mesterséges intelligenciák kiterjedt alkalmazása akár az emberiség kihalását segítheti elő azzal, hogy azok képesek lesznek felülírni az emberi parancsokat, vagy tömegesen szembefordulni azokkal. Természetesen ez nem azt jelenti, miszerint Hawking szükségesnek tartaná, hogy lemondjunk a tudományos fejlődés szükségességéről és igényéről.[9] Azt hangsúlyozta, hogy a

[5] Jobbágy Zoltán: A felkelők elleni műveletekről: Egy elfeledett klasszikus: Bernardo de Vargas Machuca, Honvédségi Szemle, 2013/2. szám pp. 15–18.

[6] Gazdag, Ferenc (szerk): Biztonsági tanulmányok – biztonságpolitika. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2011. pp. 39–40.

[7] Buzan, Barry–Waever, Ole–Wilde, de Jaap: A biztonsági elemzés új keretei. In. Póti László (szerk.): Nemzetközi Biztonsági Tanulmányok. Zrínyi Kiadó. Budapest, 2006. pp. 54–112

[8] Horrock, Chirstopher: Baudrillard és a millennium. Alexandra. (Kiadási hely és év nélkül) pp. 48–51.

[9] Ezzel kapcsolatban érdekes megjegyezni, hogy a gyógyíthatatlan idegrendszeri betegségben szenvedő Hawking speciális technológiáknak köszönheti az életben maradását és a kommunikációs képességét.

fiatalabb tudós generációknak fel kell hívni a kormányok és a társadalmak figyelmét arra, hogy az új kutatási eredményeknek milyen kockázatai lehetnek a jövőre nézve.[10] Hawking szerint ezzel elősegítenék a kutatások és technológiai fejlődés eredményeinek ésszerű kontroll alá helyezését.

A tanulmány megírásakor természetesen abból indultam ki, hogy nem csupán az új technológiák bevezetése és összekapcsolása jelenthet a társadalmakra és az infrastruktúrákra veszélyt, hanem a természeti tényezők, a környezet rombolás, a korábban alkalmazott rossz gyakorlat, vagy akár az infrastruktúrák állapotának elhanyagolása. Erre jó példát jelenthetnek a Tisza mentén az árvízi védekezés jelenlegi körülményei. A XIX. század második felében a folyószabályozás, a XX. század végén a vízgyűjtő területen a tömeges erdőirtás, az ukrajnai folyószakaszon a védművek elhanyagolása, Magyarországon a vízgyűjtők hiánya azt okozták, hogy egy olyan, egyébként több hónapig csapadékhiányos területen, mint az Alföld, az árvizekkel szemben a gátak magasításával kell védekeznünk…

A biztonság újszerű, nem a hagyományos (ti. geopolitikai és katonai) értelmezésének szükségességével a nemzeti kormányok az 1990-es években szembesültek. Az évtized végén az Egyesült Államokban az új szemléletet és eljárásmódot kifejező fogalomként a *kritikus infrastruktúra védelem* kifejezést kezdték el használni, miután Bill Clinton az Egyesült Államok elnöke 1998. május 22-én kiadta az ezzel kapcsolatos elnöki direktíváját. A dokumentumot túlzás nélkül mérföldkőnek lehet nevezni meghatározó jelentőséggel bíró infrastruktúrák és az azok által nyújtott szolgáltatások biztonsága szempontjából.

A történelem folyamán a kormányzatoknak természetesen korábban is fontos volt, hogy az alapvető infrastruktúrák működőképességét fenntartsák, hiszen ez jelentette az állam működésének egyik sarokkövét. A kritikus infrastruktúra védelem módszerét meghonosító szemléletmódban az jelentette az újszerűséget, hogy komplex módon, egységesen kezelte az úgynevezett kritikus infrastruktúrák biztonsági kockázatait.[11] Ez azért vált szükségessé, mert a különböző rendszerek kölcsönös függősége úgy növekedett, hogy az a biztonsági kihívások várható hatásait is felerősítette. Ezért a korábban alkalmazott módon, egymástól elkülönítve már nem lehetett az egyes rendszerek kockázatait kezelni.

Az új módszer- és szemléletmód, valamint az azt leképező fogalmak bevezetésének szükségességéről a szakemberek véleménye eltér egymástól. Vannak, akik szerint az 1990-es években az Egyesült Államok biztonságát fenyegető növekvő terrorfenyegetettség miatt kellett egy újszerű biztonsági intézkedéscsomagot kidolgozni.[12] Ettől eltérő álláspontra helyezkednek azok a szakértők, akik szerint az integrált biztonsági szemlélet bevezetése azért vált szükségessé, mert az egymással összekapcsolódó infrastruktúra-szektorok sérülékenységének kockázatai növekvő tendenciát mutattak.

A vizsgálatok körét ki kellett terjeszteni az újabb veszélyforrásokat jelentő egyre fejlettebb telekommunikációs rendszerekre.[13] Annál is inkább, mert az 1990-es

[10] Drámai jóslat érkezett Stephen Hawkingtól. http://tablet.hvg.hu/instant_tudomany/20160119_Dramai_joslat_erkezett_Stephen_Hawkingtol (letöltve: 2016. 01.31).
[11] Horváth, Attila: i.m.
[12] Murray, T. Alan–Grubesic, H.Tony: Overview of Reliability and Vulnerability in Critical Infrasturcture. In. Murray T. Alan–Grubesic H.Tony (eds.): Critical Infrasturcture. Reliability and Vulnerability. Springer-Verlag. Berlin, Heidelberg, New York, 2007. pp. 1–8.
[13] Protecting America's Critical Infrastructures: PDD 63. https://www.hsdl.org/?view&did=456517. p. 14. (letöltve: 2011. 03. 01.)

években már informatikai rendszereket alkalmaztak az energetikai és a közlekedési rendszerek irányításában is.

Egyik állítás igazságtartalmát sem lehet megkérdőjelezni. A fejlett országokban, az 1990-es években komoly gondot jelentett a természeti katasztrófák által okozott károk felszámolása, vagy a kritikus infrastruktúrák meghibásodásainak elhárítása, amelyek irányítási rendszerében az informatikai rendszerek egyre nagyobb szerepet töltöttek be. Ebben az időszakban drasztikus mértékben nőtt az Egyesült Államok érdekeltségei ellen annak honi területén, vagy külföldön elkövetett, súlyos következményekkel járó terrortámadások száma is.

Az Egyesült Államok ellen intézett 2001. szeptember 11-ei, stratégiai jelentőségű terrortámadás-sorozat gyökeresen változtatta meg az 1998-ban meghatározott kritikus infrastruktúra védelem politikájának szektorait, valamint az addigi szabályzó és szervezeti rendszert is. A korábbiakban elvártakhoz képest jelentős mértékben javult a köz- és magánszféra együttműködése, mert sokkal pontosabban határozták meg a szövetségi, állami és helyi szintű szervezetek, hatóságok feladatait.[14] Az egyértelmű szabályozás mellett a folyamatos, megbízható működés biztosítása érdekében a magántulajdont képező létesítmények (például olajfinomítók, kikötők, stb.) üzemeltetői számára is fontosak lettek a biztonsági kérdések.

A „9/11” néven elhíresült terrortámadás-sorozatot követően, viszonylag rövid idő múlva már a terrorfenyegetettséget nem külön kockázati tényezőként, hanem a többi, a biztonságot veszélyeztető körülménnyel együtt, komplex módon kezelték. Például 2001 őszén az anthraxot tartalmazó levélküldemények miatt fontos volt a postai szolgáltatásokra is kiterjeszteni a fokozottabb védelmet. A terrortámadások után létrehozták a Szövetségi Belbiztonsági Minisztériumot, amelynek a kritikus infrastruktúra védelmével foglalkozó szakemberei javaslatot tettek, hogy a postai küldemények biztonsági kérdéseit terjesszék ki a logisztikai rendszerekre és az ellátási láncokra is.

Az Európai Unió tagállamaiban a kritikus infrastruktúra védelem újszerű szemlélete lassan terjedt el. A közösség vezető szervezetei komoly figyelmeztető jelnek vették a 2001. szeptember 11-ei, Egyesült Államok elleni terrortámadás-sorozat tanulságait és következményeit. Ennek ellenére a kritikus infrastruktúra védelemben valódi és értékelhető előrelépés, tényleges eredményeket elérő intézkedés nem történt. Ahhoz, hogy a döntéshozatali mechanizmus ténylegesen felgyorsuljon, a 2004. március 11-ei madridi és a 2005. július 7-ei londoni közösségi közlekedés elleni terrortámadások keserű tapasztalatai kellettek. Néhány nappal azután, hogy NOB bejelentette, miszerint London nyerte el 2012-ben a XXX. Nyári Olimpiai Játékok rendezési jogát, a skóciai Gleneaglesben rendezett G8-as csúcstalálkozó idején három öngyilkos merénylő robbantotta fel magát a londoni metróban, egy pedig egy emeletes autóbuszon.

Ezután viszont Európában a terrorfenyegetettség veszélye a kritikus infrastruktúra védelemben indokolatlanul nagy hangsúlyt kapott annak ellenére, hogy hosszabb távon helytelen egy kockázati tényezőt kiemelten, a többi fenyegetettségi tényezőből kiragadva kezelni. Hiba volt a terrorfenyegetettséget évekig egyfajta primátusként kezelni, amely könnyen a más okból eredő rendkívüli események (természeti katasztrófák, működési zavarok stb.) megfelelő kezelésének rovására mehetett volna.[15]

[14] Lewis, Theodore Gyle: Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Second Edition. Jon Wiley & Sons., Haboken, New Jersey, 2015. pp. 5–25.

[15] Horváth, Attila: Terrorizmus és térjellemzők a létfontosságú rendszerelemek védelmében. In. Horváth Attila–Bányász Péter–Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési

Az Európai Unióban a kritikus infrastruktúra védelem, mint szemlélet és alkalmazható eljárásrend gyors elterjedését – a kockázati tényezők terrorfenyegetettségre való túlságos szűkítésén túl – még hátráltatta a unió közismerten lassú döntéshozatali folyamata, valamint az is, hogy az Egyesült Államokban és Európában a jelzett infrastruktúrák értelmezése eltér egymástól. Az európai gondolkodásmód az infrastruktúrákat az építményekre és létesítményekre szűkíti le, ezzel szemben az Egyesült Államokban rendszerorientált gondolkodásmód érvényesül, amelyben a létesítményeken kívül az infrastruktúrák részeként fogják fel a működtető és irányítási rendszert, a tulajdonosi és üzemeltetői szervezetet, valamint az általuk nyújtott szolgáltatásokat és az előállított árukat is. Az említett terrortámadások hatására az Európai Unió vezetőszervei 2004–2005-től kezdődően sorban adták ki a kritikus infrastruktúra védelemmel kapcsolatos irányelveket és más szabályzókat, amelyek a tagállamokat is jogszabályalkotásra kényszerítette.[16]

Az Európai Unióhoz való csatlakozásunk után Magyarországon is elkezdődött a kritikus infrastruktúra védelemmel kapcsolatos szabályzó- és intézményrendszer kialakítása, amely párhuzamosan haladt a közösségi szabályozás lépéseivel. Terjedelmi okokból a különböző munkabizottságok tevékenységének tapasztalataival és a témával kapcsolatos jogszabályalkotás folyamatával nem foglalkozom. A kritikus infrastruktúra védelem hazai szabályozásában mérföldkőnek számít, hogy az Országgyűlés 2012 novemberében elfogadta *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről* szóló CLXVI. törvényt. A törvény pontosította és az alábbiak szerint határozta meg a létfontosságú rendszerek ágazati és alágazati felosztását:

- energetika (villamosenergia-rendszer [kivéve az atomerőmű nukleáris biztonságra és sugárvédelmére, fizikai védelmére valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek], kőolajipar, földgázipar);
- közlekedés (közúti-, vasúti-, légi-, vízi közlekedés, logisztikai központok);
- agrárgazdaság (mezőgazdaság, élelmiszeripar, elosztó hálózatok);
- egészségügy (aktív fekvőbeteg ellátás, mentésirányítás, egészségügyi tartalék és vérkészletek, magas biztonsági szintű biológiai laboratóriumok, egészségbiztosítás informatikai rendszere, gyógyszer-nagykereskedelem);
- pénzügy (pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei, illetve bank- és hitelintézeti biztonság és készpénzellátás);
- infokommunikációs technológiák (információs rendszerek és hálózatok, automatikai és ellenőrzési rendszerek, internet-infrastruktúra és hozzáférés, vezetékes és mobil távközlési szolgáltatások, rádiós távközlés és navigáció, műholdas távközlés és navigáció, műsorszórás, postai szolgáltatások, kormányzati informatikai, elektronikus hálózatok);
- víz (ivóvíz-szolgáltatás, felszíni és felszín alatti vizek minőségének ellenőrzése, szennyvízelvezetés és tisztítás, vízbázisok védelme, árvízi védművek, gátak);
- jogrend – kormányzat (kormányzati rendszerek, létesítmények, eszközök, illetve közigazgatási szolgáltatások és igazságszolgáltatás);

---

rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 7–26.

[16] Erről a kérdésről lásd bővebben: Horváth Attila: i.m. (2013). Kiadvány elektronikusan elérhető az alábbi URL címen: http://mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf

– közbiztonság – védelem (rendvédelmi szervek infrastruktúrái, honvédelmi rendszerek és létesítmények).[17]

A 2012 évi CLXVI. számú törvény ún. értelmező rendelkezései meghatározzák a kritikus infrastruktúrák ágazati és horizontális kritériumait, valamint a *létfontosságú rendszerelemek*[18] védelmével kapcsolatos tevékenységek intézményi hátterét. Az ágazati kritériumok – leegyszerűsítve – a kritikus infrastruktúráknak a funkcionális feladatok szerinti csoportosítását jelentik, vagyis a jogalkotó egy korábbi kormányrendeletre alapozva abból indult ki, hogy mi a létfontosságú rendszerelemek rendeltetése. Az úgynevezett horizontális kritériumok az egyes létfontosságú rendszerelemek kiesésének az emberi életre, a természeti- és épített környezetre, illetve az infrastrukturális rendszer egészére gyakorolt várható hatásait vizsgálják. A törvény szabályozza a kijelölők, a nyilvántartók, az üzemeltetők feladatait, jog- és hatásköreit, illetve széles ellenőrzési és hatósági jogkörrel ruházza fel a BM Országos Katasztrófavédelmi Főigazgatóságát.[19]

A törvényben meghatározott szabályozási feladatok és az intézményi háttér kiépítése késedelmesen történt meg. Ezt azonban nem lehet csak BM Országos Katasztrófavédelmi Főigazgatóság terhére felróni. A késedelem oka nemcsak a jelenlegi intézményrendszerben keresendő. Jelenleg a minisztériumokban és országos hatáskörű szerveknél a biztonsági és védelmi kérdés osztályszintű szervezetek felelősségi körébe tartozik, amelyek nem tudják kellő súllyal képviselni a kritikus infrastruktúravédelem érdekeit. Ezt a véleményemet azzal is alá tudom támasztani, hogy 2006-ban a Gazdasági és Közlekedési Minisztérium Védelemkoordinációs Főosztályának megszüntetése egyszer már évekre visszavetette a problémakörrel kapcsolatos magyarországi gondolkodást.[20]

A kritikus infrastruktúrákat fenyegető és az újszerű, napjainkban még nehezen azonosítható kockázatok

Általánosságban kijelenthető, hogy a biztonsági kockázatokat csak akkor lehet elemezni és értékelni, ha már azonosítottuk őket. A kritikus infrastruktúra védelemmel foglalkozó magyarországi kutatók ezzel kapcsolatban két módszert követnek. Az egyik lényege az, hogy a lehetséges kockázati tényezőket négy-hat

[17] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny, Magyarország hivatalos lapja. 2012. évi 154. szám. pp. 26105-26106. A törvény nem nevesíti külön az ipari szektort, amelyet a korábbi jogszabály a 2080/2008 (VI.30). Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, amely az alábbi alágazatokat sorolta az ipari szektorhoz. (veszélyes anyagok előállítása, tárolása és feldolgozása, veszélyes hulladékok kezelése és tárolása /kivéve radioaktív hulladékok kezelése és tárolása/, hadiipari termelés, oltóanyag- és gyógyszergyártás - kivéve nukleáris létesítmények).

[18] A *létfontosságú rendszerelem* elnevezés sokkal jobban érthető akár a tulajdonosok, az üzemeltetők, akár a közvélemény számára, mint a kritikus infrastruktúra védelem könnyen félreérthető megnevezése. A következetesség érvényesítése érdekében azonban a jelen tanulmányban továbbra is kritikus infrastruktúra védelem kifejezést használom.

[19] Horváth Attila: Ellátási lánc, mint kritikus infrastruktúra (létfontosságú rendszerelem). In. Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 550–615. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 11.).

[20] Erről kérdésről lásd bővebben: Horváth Attila i.m.

rendező elv szerint csoportosítják (például természeti, civilizációs és egyéb veszélyforrásokra).[21] A másik módszer követői – az eddigi rendkívüli események tapasztalatai alapján és a számba jöhető fenyegetettségi tényezők elemzése után – felsorolják azokat a kockázatfajtákat, amelyek kritikus infrastruktúrák biztonságát veszélyeztetik, vagy azok kiesését okozhatják.[22]

A kockázati tényezők elemzése módszertanának tanulmányozásakor megfontolandó az Egyesült Államokban az ezredfordulót követően elterjedt gyakorlat alkalmazása. Az amerikai szakemberek szakítottak azzal a gyakorlattal, hogy csak a kockázati tényezőket kiváltó okokra koncentráljanak. A biztonságot fenyegető tényezőket együtt, komplex módon kezelik a várható káros hatásokkal együtt. Így az alábbi veszélyforrásokat különböztetik meg:

- fizikai kockázatok;
- kiber-kockázatok;
- humán kockázatok.[23]

A fizikai kockázatok körébe tartoznak a természeti és civilizációs katasztrófák. Az ún. kibertér veszélyforrásai az információs rendszereken, hálózatokon keresztül fenyegethetik a kritikus infrastruktúrákat. A humán kockázatok széleskörű veszélyforrásokat foglalnak magukba a szándékos cselekményektől (például terrortámadások, szabotázs akciók stb.) egészen a gondatlanságból, figyelmetlenségből eredő veszélyforrásokig bezárólag. Ilyen kockázat lehet például, ha egy reptéri alkalmazott felelőtlenül ad ki információkat munkahelyének biztonsági rendszeréről.

A kockázati tényezők meghatározásakor tekintettel kell lenni a fenyegetettség jellegére, az adott rendszerelem sérülékenységének összetevőire, valamint az esetlegesen bekövetkező rendkívüli események várható hatásaira. A kritikus infrastruktúrák bonyolult rendszert képeznek. Valamely, bármilyen okból bekövetkező rendkívüli esemény általában dominóhatást vált ki, amely sokszor a káresemény helyétől távol is káros következménnyel járhat. A sérülékenységet fokozza, hogy az egyes létfontosságú rendszerelemek ágazatai és alágazatai kölcsönös függőségben állnak egymással.

A kritikus infrastruktúrák biztonságát egyre nagyobb mértékben az is fenyegeti, hogy a kisebb rendszereket nagyobb rendszerekbe integrálják. Így komplex, nehezen átlátható rendszereket hoznak létre. Ma már sokszor nehéz megállapítani, hogy például az élelmiszerellátásában vajon hány termelő, feldolgozó, logisztikai vállalkozás érintett.

Néhány területen növeli a kockázatok mértékét a biztonságtudatosság hiánya, főként az olyan területeken, ahol a rendkívüli események bekövetkezésének esélye kicsi, de azok (például a egészségügyi létesítmények biztonságos üzemeltetése) súlyos következményekkel járhatnak.[24]

---

[21] Bonnyai Tünde: Úton a kritikus információs infrastruktúrák azonosítása és védelmük kialakítása felé. Hadmérnök, Budapest, VII. évfolyam 2. szám. pp. 90–105. http://hadmernok.hu/2012_2_bonnyai.pdf (letöltve: 2012. 09. 21.).

[22] Horváth, Attila–Csaba, Zágon: On the Vulnerability and Reliability of Towns and Cities. In. Csapó T.–Balogh A. (szerk.): Development of the Settlement Network in the Central European Countries: Past, Present, and Future Berlin; Heidelberg: Springer Verlag, 2012. pp. 299–312.

[23] Horváth Attila: i.m. (2013).

[24] Xu, Tie–Masys, J. Anthony: Critical Infrastructure Vulnerabilities: Embracing a Network Mindset. In:. Masys, Anthony J. (eds). Exploring the Security Landscape: Non-Traditional Security Challenges. Springer International Publishing Switzerland, 2016. pp. 177–194. DOI 10.1007/978-3-319-27914-5

A kritikus infrastruktúra védelem hosszabb távon csak akkor működhet hatékony rendszerként, ha figyelembe vesszük a közeli és távoli jövőben valószínűsíthető veszélyforrásokat is. Ez nem könnyű feladat, amelyet egy Winston S. Churchilltől származó idézettel lehet leginkább kifejezni: „*Mindig bölcs dolog előre nézni; de nehéz messzebbre tekinteni, mint ameddig ellátunk*". A Churchill által megfogalmazott „messzebbre tekintés" megéri a befektetett energiát, mert a jövőben kockázati forrást jelentő veszélyek messze túlmutathatnak a kritikus infrastruktúrák szűken vett biztonságán, azok várható geopolitikai-, társadalmi-, gazdasági, kulturális-, katonai- és egyéb vonatkozásai miatt. Ez azt jelenti, hogy nem elég csupán a jelenleg ismert kockázati tényezőkkel foglalkozni, hanem elemezni kell minden lehetséges veszélyforrást (például a technológiai fejlesztések új kihívásait).

Stephen Hawking jóslata, hogy a technológiai fejlődés az emberi civilizáció végét jelentheti, ma még nehezen képzelhető el a műszaki fejlődés trendjeivel nem foglalkozó, „hétköznapi" emberek számára. Az idősebb és a középgeneráció tagjai, – akik még használták a VHS-videokazettákat, a bakelitlemezeket felváltó CD-ket, „betárcsázós" internet kapcsolatuk volt, az 1990-es évek elején vásárolt laptopjaikon örültek annak, ha 20–25 megabájtnyi tárhellyel rendelkeztek –, össze tudják vetni, hogy egy ún. középkategóriás okostelefon is több alkalmazást képes futtatni, mint az 1990-es évek végén használt notebookok. A felsorolt példákkal csak az infokommunikációs forradalom gyors ütemének eredményeit szerettem volna érzékeltetni, de a fejlődés más területeken is elképesztő változásokat hozott.

A második világháborút követően az úgynevezett atomhatalmak a nukleáris fegyverek elterjedésével alkalmassá váltak arra, hogy akár az emberi civilizáció végét jelentő háborút vívjanak. Az 1957-ben elhunyt magyar származású matematikus zseni, Neumann János véleménye szerint is egy esetleges totális atomháború egyik legvalószínűbb következménye lehetett volna az emberiség teljes kipusztulása. A kubai rakétaválság idején az Egyesült Államok akkori elnöke, John Fitzgerald Kennedy és a környezete azzal számolt, hogy egy esetleges nukleáris háború közvetlen áldozatainak száma meghaladná a holokauszt áldozatainak számát.[25]

Az égitestek becsapódásának és az ABV-fegyverek harci alkalmazásának kockázata mellett új típusú veszélyforrásokkal kell számolni, olyanokkal, amelyek akár az emberi civilizáció egészét fenyegethetik. Ezek közé lehet sorolni a globális felmelegedés következményeit, az élelmiszertermelés és ivóvíz ellátás hiányosságait, a klímaváltozás és az üvegházhatás káros következményeit, genetikailag módosított mikroorganizmusokat, globális járványok kitörésének veszélyeit, rosszul sikerült fizikai kísérleteket, valamint a kognitív, önfejlesztő képességeket vagy rekurzívan önfejlesztő számítógépeket.[26]

A mesterséges intelligencia veszélyeire a kutatók a nemzetközi tudományos szakirodalomban már az 1950-es években felhívták a figyelmet. Az ún. „gondolkodó" gépek és robotok számtalan sci-fi regény témájául szolgáltak, nehéz is összeszámolni, hogy hány rendező forgatott igényes, de többnyire kevésbé igényes filmet Hollywood valamelyik filmstúdiójában. Az infokommunikációs technológia és a robotika fejlődési üteme miatt a mesterséges intelligencia által jelentett biztonsági és egyéb kockázatokra azonban már nem tekinthetünk úgy, mint a képzelet szüleményére. A fejlődés tendenciáit figyelve nem túlzás kijelenteni, hogy a XX. században a kézi munkaerőt felváltó ipari robotokat hamarosan kiegészítik a

[25] Metheny, G. Jason: Reducing the Risk of Human Extinction. Society for Risk Analysis, Vol. 27, No. 5, 2007. pp. 1335-1345. DOI: 10.1111/j.1539-6924.2007.00960x
[26] Metheny, G. Jason: i.m. (2007).

többfunkciós, mobilan alkalmazható robotok. A fejlődés iránya egyértelműen az, hogy a programok alapján működő rutinszerű informatikai eszközöket a kognitív, tanulásra képes informatikai eszközök fogják felváltani.[27] Ez pedig elvben azt eredményezi, hogy a számítógépek, a robotok már képesek lesznek felülbírálni a programjaikban meghatározottakat és az emberi parancsokat.

A mesterséges intelligenciák fejlődése nem csupán biztonsági kihívásokat jelent, hanem más területeken is komoly feszültséggel teli, rendszerszintű változásokat okozhat.

(A cikk második része a mesterséges intelligenciák alkalmazásának biztonsági kockázataival foglalkozik.)

FELHASZNÁLT IRODALOM

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny, Magyarország hivatalos lapja. 2012. évi 154. szám. pp. 26105–26106.

2080/2008 (VI.30). Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

Bányász Péter: A közlekedést támogató alkalmazások biztonsági aspektusai. In. Horváth Attila–Bányász Péter–Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 47–60.

Bányász Péter: A közösségi média szerepe a kasztrófaelhárításban a Sandy-hurrikán példáján. In. Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből II., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 135–148.

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekinttel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In.: Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 643–672. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 11.).

Barabási Albert László: Behálózva. (Második, bővített és átdolgozott kiadás.) Helikon Kiadó, Budapest, 2008. 320 p.

Baudlliard, Jean: Az utolsó előtti pillanat. (A közönyös paroxista). Beszélgetések Philippe Petit-vel. Magvető Kiadó, Budapest, 2000. 148 p.

Beckstead, Nick–Bostrom, Nick–Bowerman, Niel–Cotton-Barratt, Owen–MacAskill, William–Ó hÉgearttaigh, Seán–Ord, Toby: Unprecedented Technological Risks. Global Proorities Project. k.h.n., 2014. 12 p.

Bonnyai Tünde: Úton a kritikus információs infrastruktúrák azonosítása és védelmük kialakítása felé. Hadmérnök, Budapest, VII. évfolyam 2. szám. pp. 90–105. http://hadmernok.hu/2012_2_bonnyai.pdf (letöltve: 2012. 09. 21.)

Buzan, Barry–Waever, Ole– Wilde, de Jaap: A biztonsági elemzés új keretei. In Póti László (szerk). Nemzetközi Biztonsági Tanulmányok. Zrínyi Kiadó. Budapest, 2006. pp. 54–112.

[27] Doorn van, Menno–Bloem, Jaap–Duivestein, Sander– Ommeren van, Erik: Machine Intelligence. Sogeti, Creative Commons, k.h.n. k.é.n, pp. 6-7. https://www.sogeti.nl/sites/default/files/VINT-rapport%20Machine%20Intelligence.pdf (letöltve: 2016. 05. 09.).

Canneti, Ellias: Tömeg és hatalom. Európa Könyvkiadó, Budapest, 1991. 497 p.
Coaffe, Jon–Wood, Murakami–Davdl Rogers, Peter: The Everyday Resilience of the City. Palgrave Macmillen, New York and London. 2009. 343 p.
Degryse, Christophe: Digitalisation of the economy and its impact on labour markets Working Paper. 2016. European Trade Union Institute. Brussels, 2016. https://www.researchgate.net/profile/Christophe_Degryse/publication/297392058_Digitalisation_of_the_economy_and_its_impact_on_labour_markets/links/56debb3808aeb8b66f95f7a8.pdf
Diamond, Jared: A harmadik csimpánz felemelkedése és bukása. (Második kiadás) Typotex, Budapest, 2009/a. 416 p.
Diamond, Jared: Összeomlás. Tanulságok a társadalmak továbbéléséhez. (Második kiadás) Typotex, Budapest, 2009/b. 577 p.
Doorn van, Menno–Bloem, Jaap–Duivestein, Sander–Ommeren van, Erik: Machine Intelligence. Sogeti, Creative Commons, k.h.n. k.é.n, 40. p. https://www.sogeti.nl/sites/default/files/VINT-rapport%20Machine%20Intelligence.pdf (letöltve: 2016. 05. 09.).
Fjäder, O. Chirstian: National Security in a Hyper-connected World. Global Interdependence and National Security. In. Masys, J Anthony (ed.): Exploring the Security Landscape: Non-Traditional Security Challenges. Springer, pp. 31-58. DOI 10.10007/978-3319-27914-5. (letöltve: 2016. 04. 02.).
Földi László: Az éghajlatváltozás hatása a biztonságra és a katonai erő alkalmazására, a hadviselés ökológiai kérdései. In. Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 550–615. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 23.).
Gazdag Ferenc (szerk): Biztonsági tanulmányok – biztonságpolitika. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2011. 414 p.
Haig Zsolt–Várhelyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest 286. p.
Horrock, Chirstopher: Baudlliard és a milleneum. Alexandra. (Kiadási hely és év nélkül)
Horváth, Attila–Csaba, Zágon: Critical Transport Infrastructure Protection: A Reserach on the Security of the Supplay Chains. Economics and Management 2015. pp. 47–54. (2015).
Horváth, Attila–Csaba, Zágon: On the Vulnerability and Reliability of Towns and Cities In Csapó T.–Balogh A. (szerk.): Development of the Settlement Network in the Central European Countries. Past, Present, and Future. Berlin–Heidelberg. Springer Verlag, 2012. pp. 299–312.
Horváth Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. In. Horváth, Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből I., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 25–48.
Horváth, Attila: ellátási lánc, mint kritikus infrastruktúra (létfontosságú rendszerelem) In. Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 550–615. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 11.).

Horváth Attila: Terrorizmus és térjellemzők a létfontosságú rendszerelemek védelmében. In. Horváth Attila–Bányász Péter–Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014/a. pp. 7–26.

Horváth, L. Attila: A terrorizmus csapdájában. Zrínyi Kiadó, Budapest, 2014. 287 p.

http://www.automationsmaland.se/dokument/BCG_The_Robotics_Revolution_Sep_2015.pdf (letöltve: 2016. 04. 21.).

Jobbágy Zoltán: A felkelők elleni műveletekről. Egy elfeledett klasszikus: Bernardo de Vargas Machuca. Honvédségi Szemle, 2013/2., pp. 15–18.

Jobbágy, Zoltán: A háború antropológiája: primitív hadviselés, gerilla hadviselés és a szövetséges összhaderőnemi műveletek sikere. Hadtudomány: XXV, évfolyam 2015. E-szám pp. 67–78.

http://www.mhtt.eu/oldsite/hadtudomany/2015/2015_elektronikus/index.html

Jobbágy, Zoltán: Biztonságpolitika, haderőreformok. A humánerőforrás-gazdálkodás katonai életpályával összefüggő kérdései. Hadtudomány. 2015. évi különszám. pp. 30–40.

Kis-Benedek József: Az Iraki és Levantei Iszlám Állam (ISIL) és az ellene folytatott küzdelem tendenciái. Hadtudomány, 2016/1–2. szám. pp. 29–39.

Kovács László–Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság III. évfolyam 1. szám, 2010. február, pp. 44–56.

Learning from the Blackouts. Transmission System Securityin Competitive Electricity Markets. International Energy Agency and OECD, Paris, 2005. 216 p. http://www.iea.org/publications/freepublications/publication/blackouts.pdf (letöltve: 2016. 03. 19.).

Lewis, Theodore Gyle: Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Second Edition. Jon Wiley & Sons., Haboken, New Jersey, 2015. 399 p.

Little, G. Richard: Managing the Risk of Cascading Failure int the Complex Urban Unfrastructures. In.: Graham Stephen (ed). Disrupted Cities. Routledge, Taylor& Francis Group. New York, London, 2010. pp. 27–39.

Macaulay, Tyson: Critical Infrastructure: Understanding its Component Parst, Vulnerabilities, Operating Risks and Interdepencies. CRC Press. New York, London, 2009. 320 p.

Metheny, G. Jason : Reducing the Risk of Human Extinction. Society for Risk Analysis, Vol. 27, No. 5, 2007. pp. 1335-1345. DOI: 10.1111/j.1539-6924.2007.00960x

Molnár Ferenc: A magyar társadalom biztonságról, védelemről alkotott képe és a kritikus infrastruktúra. In. Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből I., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 107–127.

Murray, T. Alan–Grubesic, H.Tony: Overview of Reliability and Vulnerability in Critical Infrasturcture. In. Murray T. Alan–Grubesic H. Tony (eds.): Critical Infrasturcture. Reliability and Vulnerability. Springer Verlag. Berlin, Heidelberg, New York, 2007. pp. 1–8.

Müller, C. Vincent: ‘Editorial: Risks of artificial intelligence’. In. Vincent C. Müller (ed.): Risks of general intelligence. London, CRC Press – Chapman & Hall, 2016 pp. 1–8. http://www.sophia.de/pdf/2015_AI-Risk_Editorial.pdf (letöltve: 2016. 05. 21.).

New Robot Strategy. Japan's Robot Strategy Vision, Strategy, Action Plan. The Headquarters for Japan's Economic Revitalization. k.h.n., 2015 URL cím: http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf (letöltve: 2016. 04. 18.)

Orbók Ákos: Az okosváros közlekedés irányításának kihívásai. In. Horváth Attila–Bányász Péter–Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 121–128.

Pacione, Michael: Urban Geography. A Global Perspective. Routledge, Taylor& Francis Group. New York, London, 2009. 703 p.

Petkovics Tamás: A hadiipar fejlesztési lehetőségei Magyarországon. Katonai Logisztika. 24. évfolyam, 1 szám. 2016. pp. 54–87.

Porkoláb Imre: Az innováció hatása a hadviselésre. Hadtudomány, 2016/1–2. szám. pp. 19–27.

Porkoláb Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány, 2015/3–4. szám. pp. 36–48.

Protecting America's Critical Infrastructures: PDD 63. https://www.hsdl.org/?view&did=456517. p. 14. (letöltve: 2011. 03. 01.)

Sirkin, L. Harold–Zinser, Michael–Rose, Justin Ryan: The Robotics Revolution. The Next Great Leap in Manufacturing. The Boston Consulting Group, Boston, 2015.

Szászi, Gábor: A vasúti közlekedési alágazat, mint kritikus infrastruktúra. In. Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből II., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 5–32.

Szenes Zoltán: Tudomány és a korszerű haderő. Magyar Tudomány. 2015/2. szám. pp. 194–201.

Walt, M. Stephen: A biztonsági tanulmányok reneszánsza. In. Póti László (szerk.): Nemzetközi biztonsági tanulmányok. Zrínyi Kiadó, Budapest, 2006. pp. 9–52.

Xu, Tie–Masys, J. Anthony: Critical Infrastructure Vulnerabilities: Embracing a Network Mindset. In. Masys, Anthony J. (eds.): Exploring the Security Landscape: Non-Traditional Security Challenges. Springer International Publishing Switzerland, 2016. pp. 177–194. DOI 10.1007/978-3-319-27914-5.